Escuela Politécnica Superior

Desarrollo de un sistema de adquisición 3D del cuerpo humano e implementación de medidas de Seguridad y protección de datos

Grado en Ingeniería Informática

Trabajo Fin de Grado

Autor:
José Carlos Jurado García

Tutor/es:
Marcelo Saval Calvo

Andrés Fuster Guilló

Universitat d'Alacant
Universidad de Alicante

Julio 2020

UNIVERSIDAD DE ALICANTE

Departamento de Tecnología informática y Computación

Trabajo de Fin de Grado

Desarrollo de un sistema de adquisición 3D del cuerpo humano e implementación de medidas de seguridad y protección de datos

José Carlos Jurado García

Tutores

Dr. Marcelo Saval Calvo

Dr. Andrés Fuster Guilló

Memoria presentada para aspirar al grado de:

GRADUADO EN INGENIERÍA INFORMÁTICA

Alicante, 30 de Julio de 2020

“A veces la vida te golpea en la cabeza con un ladrillo. No pierdas la fe.”

Steve Jobs.

Agradecimientos

En esta sección quisiera agradecer a todos aquellos que me han apoyado haciendo más llevadera mi vida universitaria.

Principalmente, quisiera dar las gracias a mi abuela y a mi madre, por todo el sacrificio, compresión, y amor incondicional que he recibido, por los buenos momentos compartidos y por los valores que me habéis transmitido.

A mi pareja y compañera de batallas en este Grado de Ingeniería Informática, Ruth, uno de mis pilares durante toda la carrera. Infinitamente agradecido por estar ahí para aguantarme en todo momento , incluso en la peor etapa de mi vida.

También a esos compañeros y amigos conocidos en este grado tales como: Arturo, Bernadette, Luis, Verónica, Francisco y Alberto. Gracias a todos por estar ahí permitiéndome mejorar tanto en los estudios como en lo personal, se me quedarán grabados a fuego esos momentos del futbolín en el Club Social 3, las escapadas a la bolera o el outlet, y como no, el grupo de estudio que realizábamos y que, en gran medida, me permite estar redactando este trabajo.

A mis mejores amigos Xisco, José Juan y Efrén, por toda la compresión y por ayudarme a eliminar el estrés cuando este se apoderaba de mí y por celebrar conmigo todos mis logros.

A todos los profesores que me han impartido clase a lo largo del grado, dándome la posibilidad de obtener uno de los bienes más preciados de este mundo, conocimiento, en especial a Andrés Fuster, Jorge Azorín y José Ángel Berná, sin olvidarme de uno de los mejores profesores que he tenido la suerte de conocer, José Manuel Baldo, el cual fue un apoyo constante cuando tuve la necesidad.

Por último, a todos mis compañeros del proyecto Marcelo Saval, Víctor Villena y Rafael Olid, por darme la oportunidad y los conocimientos que me han permitido realizar este trabajo.

Y te agradezco que tengas este trabajo en tus manos.

Resumen

En este documento se presenta mi trabajado de fin de grado, el cual se enmarca en un proyecto de investigación llamado Tech4Diet, cuyo título es "Modelado y visualización 4D del cuerpo humano para la mejora de la adherencia al tratamiento dietético-nutricional", cuya referencia es "TIN2017-89069-R". En este proyecto se busca mejorar los procesos actuales para el tratamiento de la obesidad mediante la implantación de un modelo de visualización 4D del cuerpo humano para el análisis de la evolución morfológica. Este modelo 4D podrá ser visualizado mediante realidad virtual inmersiva y simulaciones de la evolución consecuencia del tratamiento.

El presente trabajo aborda dos procesos muy diferentes, en primer lugar, el desarrollo de un sistema de adquisición 3D para extraer representaciones del cuerpo humano mediante el uso sensores RGB-D, y, en segundo lugar, la realización de un estudio de las medidas de seguridad que son de obligatoria aplicación en el proyecto para cumplir la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

Los sensores o cámaras RGB-D son dispositivos que nos dan la posibilidad de obtener la información de color y de profundidad de la escena capturada. Estos sensores despiertan una intensa actividad investigadora en múltiples áreas, cuyos resultados ya se están haciendo notar en todo el mundo. En este trabajo se aborda el análisis, diseño e implementación de un sistema de adquisición multicámara 3D del cuerpo humano a partir de sensores RGB-D. Los componentes y herramientas utilizadas para el desarrollo y puesta en marcha de este sistema han sido elegidos cuidadosamente para completar los objetivos del proyecto.

Además de la descripción de las herramientas y dispositivos, aquí se presentan los módulos desarrollados para la adquisición multicámara, así como experimentación del funcionamiento.

Es fundamental hoy en día tener en cuenta que el sistema del proyecto obtiene y almacena datos de carácter personal, así como información del paciente e información que corresponde al ámbito de la salud. Por este motivo es de carácter obligatorio que se implementen ciertas normativas de seguridad para poder cumplir con la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales. Para el cumplimento de esta

ley se realiza un estudio del Esquema Nacional de Seguridad, así como un plan de adecuación, el cual servirá al proyecto para saber dónde tiene que enfocar sus esfuerzos, por lo que a seguridad se refiere.

Índice General

Índice de figuras

Índice de tablas

1. Introducción

En este primer capítulo se van a incluir la motivación y contexto del proyecto, donde se proporcionará el marco general de este estudio. Además, se presentará el marco metodológico en el cual se describirá el contexto del proyecto y sus procesos debido a la cantidad de campos que se tocan, desde la de implementación de código hasta la parte de gestión de seguridad. Por último, se plantean los objetivos generales del proyecto.

1.1. Motivación y contexto

Siempre me he sentido atraído por la tecnología, pero no fue hasta los 14 años cuando empecé a trastear con el dispositivo Kinect de Microsoft, una cámara RGB-D distribuida principalmente para la consola XBOX 360. En ese momento comprendí que la informática era mi pasión y no un simple hobby, además, debido a este cambio de mentalidad, mi mente se llenó de dudas sobre la posibilidad de uso y funcionamiento de las herramientas que están disponibles para todo el público. Estos sucesos en mi adolescencia fueron los precursores para realizar un proyecto de fin de carrera orientado, principalmente, al ámbito de visión por computación.

Años después, en la universidad, comencé a informarme sobre este campo de investigación, sobre todo la parte del uso de la visión por computación en el ámbito de coches autónomos o en el de reconocimiento facial, intentando obtener los conocimientos necesarios para formarme y emprender en este ámbito en el futuro.

Posteriormente, en la asignatura de Ingeniería de los Computadores, en el segundo curso del grado, Andrés Fuster Guillo y Jorge Azorín me dieron la oportunidad de unirme a su grupo de investigación, orientado al área de visión por computación, la cual me interesaba desde tiempo atrás. En este grupo he tenido la suerte de trabajar con profesionales en este ámbito formando equipo con Marcelo Saval y Víctor Villena, además de varios compañeros de la carrera.

Una vez en el proyecto descubrí la trayectoria del equipo de trabajo, iniciado por Andrés con la tesis “Modelado de sistemas para visión realista en condiciones adversas y escenas sin estructura” (Fuster Guilló, 2004) en la que proporciona métodos para minimizar los efectos de una imagen de baja calidad en situaciones donde no es posible

distinguir los elementos que aparecen, por ejemplo, objetos que se sitúan en una zona de penumbra o que deslumbre al propio objeto.

Siguiendo la misma línea de problemas de visión en condiciones adversas, Jorge Azorín, con su tesis "Modelado de sistemas para visión de objetos especulares. Inspección visual automática en producción industrial" (Azorín López, 2008), propone diferentes métodos para mejorar la inspección visual automática en situaciones donde haya escenas especulares.

Además, en la misma línea, pero con datos tridimensionales, Marcelo Saval propone en su tesis "Methodology based on registration techniques for representing subjects and their deformations acquired from general purpose 3D sensors" (Saval Calvo, 2015) un conjunto de métodos con los que pretende mejorar la adquisición de datos 3D a través de cámaras o sensores RGB-D en condiciones adversas.

También Víctor Villena en su proyecto de fin de carrera, titulado "Análisis comparativo de métodos de calibrado para sensores RGB-D y su influencia en el registro de múltiples vistas" (Villena Martínez, 2015), realiza un análisis donde prueba diferentes métodos de calibrado para los sensores RGB-D y se comparan diferentes vistas en un sistema de registro global.

Mi incorporación a este equipo de investigadores se debe a la necesidad de desarrollar trabajos de investigación e implementación para un proyecto llamado Tech4Diet cuyo título es "Modelado y visualización 4D del cuerpo humano para la mejora de la adherencia al tratamiento dietético-nutricional" y cuya referencia es "TIN2017-89069-R", el cual está subvencionado por el Fondo Europeo y la Agencia Estatal de Investigación (AEI) de España. En este proyecto se busca mejorar los procesos actuales para el tratamiento de la obesidad mediante visión artificial (Fuster Guilló et al., 2019).

1.2. Marco metodológico y tecnológico. Tech4Diet

Como se ha explicado de forma breve en el apartado anterior, el proyecto se enmarca en la mejora del tratamiento de la obesidad aprovechando el potencial de áreas tecnológicas como la realidad virtual o la visión por computación, dicho esto, el objetivo principal del proyecto Tech4Diet es el desarrollo de un modelo de representación 4D (Modelado 3D + Tiempo) del cuerpo humano, lo que concede la

posibilidad de crear un registro de modelos del cuerpo en diferentes instantes del tiempo, permitiendo al paciente visualizar de manera realista la evolución de su cuerpo en el tiempo, incentivando al paciente a continuar con el tratamiento, aumentando así su motivación y su adherencia a este.

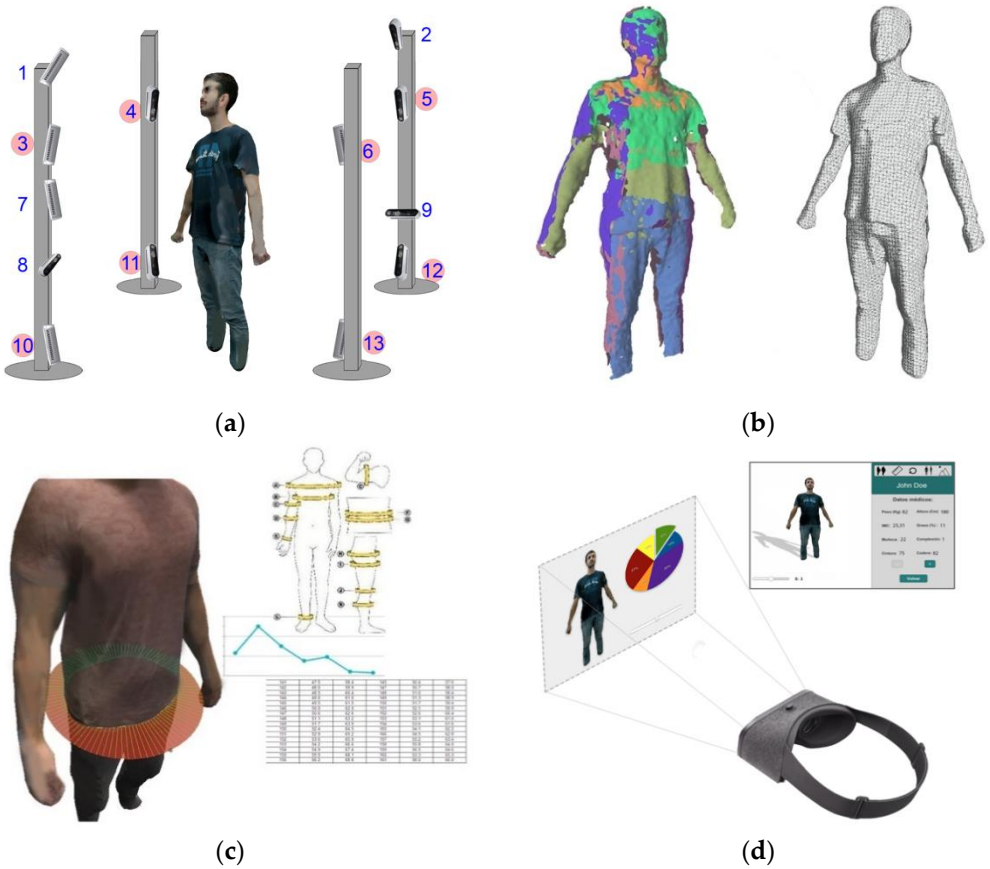

Figura 1. Sistema de red de cámaras propuesto(a). Modelos corporales: Nube de puntos y mallado. Medición del cuerpo 3D (c) y representación dispositivos de realidad virtual (d).

Con ello, se permitirá a los propios investigadores del ámbito nutricional la posibilidad de realizar comparaciones, análisis de evolución en las diferentes fechas donde se realicen la adquisición de datos y análisis de la eficacia de los tratamientos disponibles, debido a que se podrán recoger medidas y datos que previamente no se podían tomar, por tener el modelo real de la persona el sobre el que tomar nuevas medidas.

El proyecto sigue tres líneas de investigación y desarrollo, necesarias para la consecución de los objetivos del proyecto, que son la adquisición, el modelado 3D y 4D, y la visualización de datos del modelo humano (ver Figura 1). Estos son los procesos técnicos en los que se forma el proyecto. Estos tres se explican más detalladamente a continuación:

- Fase de Adquisición.

  Es el proceso donde se obtienen todos los datos necesarios para el modelado 3D del cuerpo humano del paciente, que se realizará en la siguiente fase. Para poder realizar esta fase se decidió utilizar múltiples sensores desde diferentes lados, por lo que era necesario montar una especie de cabina formada por cuatro columnas de aluminio en las que se sujetan de 8 a 13 sensores RGB-D Realsense de Intel que se utilizan para captar todo el cuerpo del paciente, como se puede apreciar en la siguiente figura (ver Figura 1 y Figura 2).

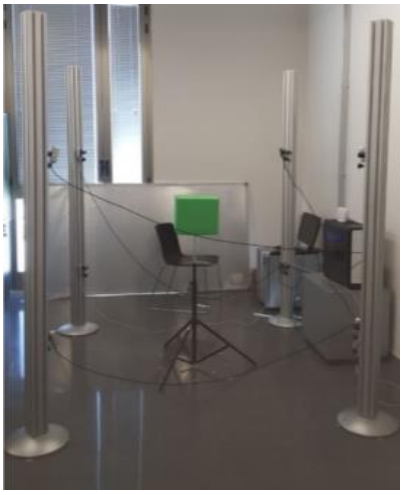

Figura 2. Cabina Adquisición

  Para obtener los datos del modelado 3D, que se explicará en la siguiente fase, es necesario realizar varios procesos. Para empezar, se realizar la fase de calibrado en la que se ajustarán los todos los sensores de manera intrínseca y extrínseca. A continuación, en la fase de adquisición, se registrarán tres tipos de datos: la imagen de color, los datos de profundidad y la nube de puntos. Finalmente, en la fase de procesado y registro se optimizan y se aplican transformaciones a las nubes de puntos para generar un registro de estas, obteniendo el cuerpo 3D completo en un instante de tiempo.

- Fase de Modelado.

  En esta fase se desarrolla un sistema de modelado en el cual se utilizan los datos recogidos en la fase anterior para poder generar una malla con textura (ver Figura 1b). La malla se genera a partir del registro de las nubes de puntos, utilizando el algoritmo matemático de Poisson y se le dará

textura proyectando las imágenes de color obtenidas previamente de los sensores RGB-D (ver Figura 3).

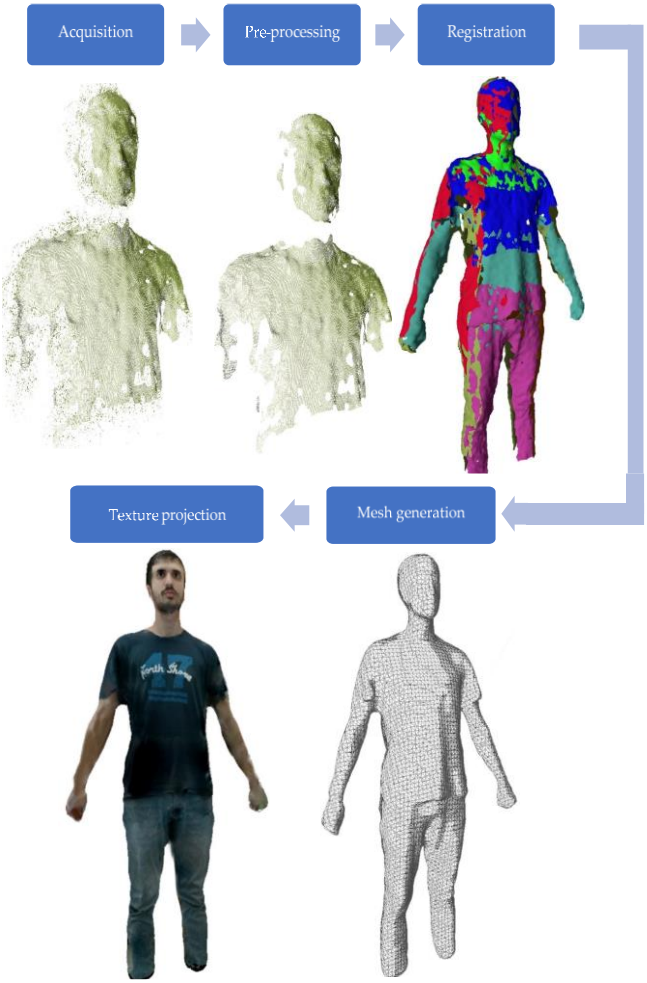

Figura 3 Procesos de la reconstrucción 3D

- Fase de Visualización.

  Como se ha comentado previamente, en esta fase se realiza un sistema de visualización de los datos 3D, el cual será usado tanto por el paciente para mejorar la adherencia al tratamiento con un aumento de entusiasmo (ver Figura 1d), como por el médico para permitirle observar la evolución temporal del paciente y la toma de medidas precisas de la salud del paciente (ver Figura 1c y Figura 4).

Figura 4. Programa de visualización

Por último, hay que tener en cuenta que en todas las fases del proyecto se manejan datos de carácter personal de los pacientes que utilicen el servicio ofrecido por Tech4Diet. Por este motivo, se deben cumplir, en todo momento, las normativas de la LOPDGDD (Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales) la cual exige aplicar el ENS (Esquema Nacional de Seguridad) de España para poder salvaguardar los datos y el sistema del proyecto.

Dentro de todos los retos que se afrontan en el proyecto Tech4Diet en los que he participado, han sido, primeramente, el desarrollo del sistema encargado en la adquisición de datos 3D y posteriormente, la implementación de las medidas de seguridad necesarias para cumplir la LOPDGDD y el ENS.

1.3. Objetivos

Este trabajo tiene dos objetivos generales: desarrollar un sistema de adquisición 3D multicámara; estudio de medidas LOPDGDD que deban cumplirse tanto a la adquisición como en el total del proyecto Tech4Diet.

Se plantean los siguientes objetivos concretos:

- Analizar y definir el sistema de adquisición con el fin de implementar un sistema modularizable y escalable.
- Desarrollo de un sistema de adquisición de datos 3D utilizando los sensores Realsense D435.
- Investigar las medidas exigidas por la LOPDGDD.
- Investigar e implementar las medidas de seguridad exigidas por el ENS.

1.4. Estructura del documento

Este proyecto tiene tres capítulos en los que se enmarca todo el trabajo realizado durante mi estancia en el proyecto, los cuales expondré brevemente a continuación:

- Adquisición Multicámara RGB-D.

  En este capítulo se explicará, en primer lugar, el entorno de desarrollo utilizado para el sistema de adquisición, explicando principalmente los

tipos de sensores 3D sin contacto que hay actualmente, en segundo lugar, se detallará el sensor escogido y el hardware y software utilizados para este desarrollo.

Por último, el diagrama de clases desarrollado en el proyecto para poder implementar un sistema modular y escalable, y se explica brevemente ciertas partes esenciales del código del sistema de adquisición junto con los resultados obtenidos en este proceso.

- Seguridad y Protección de Datos.

  En el segundo capítulo se explicará porqué se debe implementar medidas de seguridad para cumplir la LOPDGDD, así como un breve resumen de lo que trata esta ley. Además, se detallan que tipos de tratamientos o usos se pueden realizar con estos datos.

  Para finalizar, se realizará un estudio del ENS y se implantará el plan de adecuación exigido por esta normativa y que servirá como guía para la implementación de las medidas necesarias para salvaguardar tanto el sistema del proyecto como los datos obtenidos de los pacientes.

- Conclusión.

  En este último capítulo se explicarán las conclusiones que han sido obtenidas tras realizar las tareas en el proyecto Tech4Diet, así como las líneas futuras, con el fin de mejorar y optimizar el sistema adquisición y el apartado de seguridad. Por último, se expondrán las conclusiones personales que he obtenido después de realizar este trabajo en el proyecto.

2. Adquisición Multicámara RGBD

Como se ha puesto de manifiesto en la introducción, este es un proyecto en el que utilizamos sensores 3D para capturar el contorno de un individuo para poder hacer estudios y obtener resultados de los tratamientos realizados al paciente.

Es este capítulo se tratará lo esencial para la adquisición multicámara, desde las decisiones tecnológicas, en cuanto a software y hardware se refiere, hasta a las decisiones técnicas en el desarrollo del sistema de adquisición multicámara, que servirá para cumplir los objetivos generales del proyecto.

2.1. Entorno de desarrollo

En este apartado se van a desarrollar las decisiones tomadas en cuanto a los sistemas tecnológicos, software y hardware, disponibles en el mercado, los cuales servirán para realizar las tareas y cumplir con los objetivos marcados.

2.1.1. Sistemas de visión 3D

Como se ha expuesto en el capítulo anterior, para la adquisición de datos del individuo se utiliza una tecnología de visión 3D a distancia, por este motivo es necesario ver que sensores existen actualmente en el mercado y cual sirve, en términos de calidad/precio, para el propósito del proyecto.

- TOF (Time-of-Flight).

  Permite estimar la distancia entre el sensor y el cuerpo, calculando el tiempo transcurrido entre la emisión y la recepción de un haz de luz infrarrojo (Cui et al., 2010).

- Cámaras estereoscópicas.

  Tecnología que utiliza dos o más cámaras calibradas para estimar la profundidad, esta estimación se realiza calculando la disparidad de las imágenes que se obtienen de cada cámara, con esta se puede obtener la distancia (Lazaros et al., 2008).

- Luz estructurada.

  Sensor que permite capturar la forma y características de un objeto, mediante la proyección de un patrón conocido de luz y calcula la deformación realizada por el objeto. Uno de los principales problemas es

la necesidad de saber la distancia que hay entre el sensor y el objeto (Gu et al., 2014).

- LIDAR (Laser Illuminated Detection and Ranging).

  Sensor que permite determinar la distancia y el mapa de profundidad desde aquel a una superficie. Estos datos se obtienen proyectando un haz láser sobre la superficie y analizando la reflexión del pulso (Schwarz, 2010).

- Sensores RGB-D.

  Sensores que combinan sensores de detección de profundidad con cámaras de color, para proporcionar de manera simultánea el mapa de profundidad y el color del objeto o superficie (Khoshelham & Elberink, 2012).

a. *LIDAR*

b. *ToF*

c. *Luz estructurada*

d. *Estereoscópica*

e. *RGB-D (Color y ToF)*

Figura 5. Sensores 3D

De todas estas tecnologías de visión 3D a distancia, se decide utilizar los sensores RGB-D debido, entre otros, a los siguientes detalles: Son sistemas de bajo coste, lo que

implica una posibilidad de transferencia de mercado; Son portables debido a su tamaño reducido; Y proporciona un sensor de profundidad y uno RGB.

Hoy en día existe un catálogo de marcas que ofrecen dispositivos RGB-D de bajo coste, por lo que una de las principales problemáticas era la decisión del dispositivo que iba a ser el utilizado para el desarrollo inicial del proyecto.

La decisión sobre que sensor RGB-D, de todos los que existen actualmente, iba a ser el adecuado para realizar las tareas de adquisición, fue influida tanto a la relación calidad/precio como a la resolución de captura de las cámaras, ya que hay diferentes marcas conocidas como Intel y Microsoft, y otras no tan conocidas como Orbbec y Primesense, que ofrecen este tipo de sensores y que sirven para la finalidad del proyecto (ver Figura 6).

Figura 6. Sensores RGB-D

Esta comparación se puede ver en la siguiente tabla en la cual se realiza un estudio de las diferentes resoluciones de las capturas a color y las capturas de profundidad, así como el precio y Campo de visión (FOV) de los sensores RGB-D que hay en el mercado actualmente.

Nombre	Precio €	RGB	Profundidad	FOV
Kinect v2	199.99	1920x1080	512x424	70x60
Orbbec Astra S	149.99	640 x 480	640 x 480	60x49
Orbbec Astra Pro	149.99	1280 x 720	640 x 480	60x49
Realsense D415	149.00	1920x1080	1280x720	69x42
Realsense D435	**179.00**	**1920x1080**	**1280x720**	**85x58**
Primesense Carmine	295.00	1280x960	640x480	54x45

Tabla 1. Comparativa sensores RGB-D

El dispositivo elegido fue la Realsense D435, el cual era superior a los otros dispositivos, tanto en resolución RGB y profundidad como en el apartado del campo de visión, además, utiliza una conexión tipo C que permitirá transmitir los datos a una velocidad de 4,8Gbps (ver Figura 7).

Figura 7. Realsense D435

Así mismo, los sensores de la gama Realsense D400 están pensados para poder utilizar múltiples dispositivos y realizar capturas simultaneas, ya sea una orientación hacia fuera, pudiendo capturar la profundidad de la parte frontal y posterior de la situación física de las cámaras, o una orientación interna, que se utilizará en el proyecto, pudiendo capturar todos los lados del objeto enfocado. Estas dos orientaciones las podemos ver en la siguiente figura (ver Figura 8)

Figura 8. Posibles orientaciones Realsesne D400

Por estos motivos, se ha decido utilizar el sensor Realsense D435 para el desarrollo inicial del proyecto (Grunnet-Jepsen et al., 2018).

2.1.2. Herramienta de desarrollo software

En el desarrollo del software del sistema de adquisición multicámara se han utilizado diversas herramientas, tanto para el desarrollo como para su mantenimiento y gestión: Bitbucket para el control de versiones, Atom como IDE y el lenguaje C++ y el Software Development Kit (SDK) de Intel para las cámaras Realsense D400 (ver Figura 9).

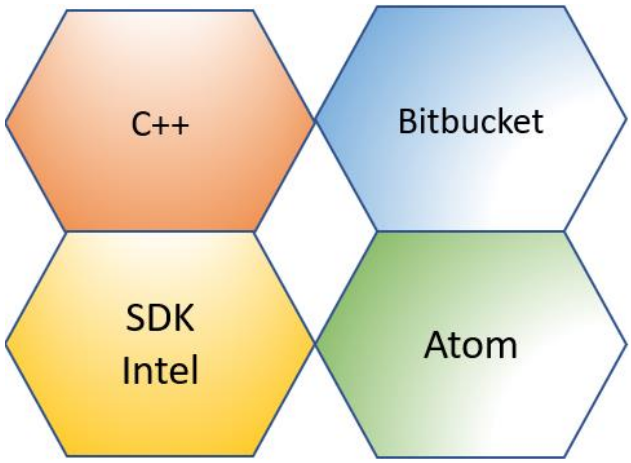

Figura 9. Herramientas Software utilizadas

La tecnología utilizada para la implementación del código de adquisición es el SDK, que proporciona Intel para sus dispositivos Realsense desde su repositorio en la página de GitHub. Para ser más específico, se ha utilizado la versión 2.0 de este SDK, en el que proporciona la posibilidad de programar en los lenguajes de programación, C++ y Python y en los sistemas operativos Linux y Windows. Además, aporta wrappers para diferentes lenguajes de programación como Unity, OpenCV, Node.js, Matlab, Unreal Engine; lo que nos permitirá poder trabajar con estas herramientas si fuese conveniente. También nos permite utilizar aplicaciones de terceros como SQLITE, OPENGL e IMGUI.

Figura 10. Logo Intel Realsense

Por lo que respecta al proyecto, toda la implementación ha sido desarrollada en un sistema operativo Ubuntu 16.04 LTS utilizando el lenguaje C++, ya que es el lenguaje con el mayor aporte comunitario, de los lenguajes disponibles, para las cámaras Realsense D435.

2.1.3. Red de conexión multicámara

Para la estructura donde se van a colocar los dispositivos Realsense D435 es necesario tener un cable de conexión lo suficientemente largo como para conectar los dispositivos al servidor donde se ejecutará la aplicación, ya que los cables que vienen con el sensor tienen una longitud insuficiente para ser utilizado en esta estructura.

El problema principal se origina en que la cámara envía una gran cantidad de datos, por lo que un cable USB con conexión tipo C, en uno de los extremos, y con un tipo A 2.0 ,en el otro, pueda generar un cuello de botella a la hora de trasmitir los datos, por este motivo se debía que asegurar que tuvieran un tipo A 3.0, además fue necesario adquirir dos tarjetas de expansión USB con controladoras individuales ya que esto también reducía la cantidad de datos transferidos.

Después de un análisis de mercado se descubrieron dos cables que cumplían los requisitos, uno de la marca iVolver y otro de la marca NewNex, estos cables se pueden encontrar en la página web de Amazon, la gran diferencia que existe entre los dos es la disparidad de precios, la duración de vida y el testeo con la Realsense. El precio de la marca iVolver para este tipo de cables era inferior a 3 euros por unidad, mientras que la marca NewNex tiene un precio de 51€ por unidad, aunque aseguran una duración de vida útil mucho mayor que el de la marca iVolver e incluso muestran el funcionamiento eficiente de sus cables con la Realsense D435 en su página oficial. Aún con estas diferencias, elegimos los cables de la marca iVolver, ya que para una etapa de desarrollo inicial es permisible que la vida útil del cable sea inferior.

2.2. Desarrollo de aplicación

En este apartado se van a desarrollar todas las decisiones en cuanto a implementación del software de adquisición multicámara utilizando el SDK de Realsense y el lenguaje de programación C++, como se ha expuesto previamente.

2.2.1. Diagrama de clases

Al inicio del desarrollo se pudo apreciar la necesidad de realizar un diagrama de clases para poder distribuir el código, ya que la complejidad crecería y dificultaría el mantenimiento y la modificación del propio código en un futuro. Este diagrama se explica continuación:

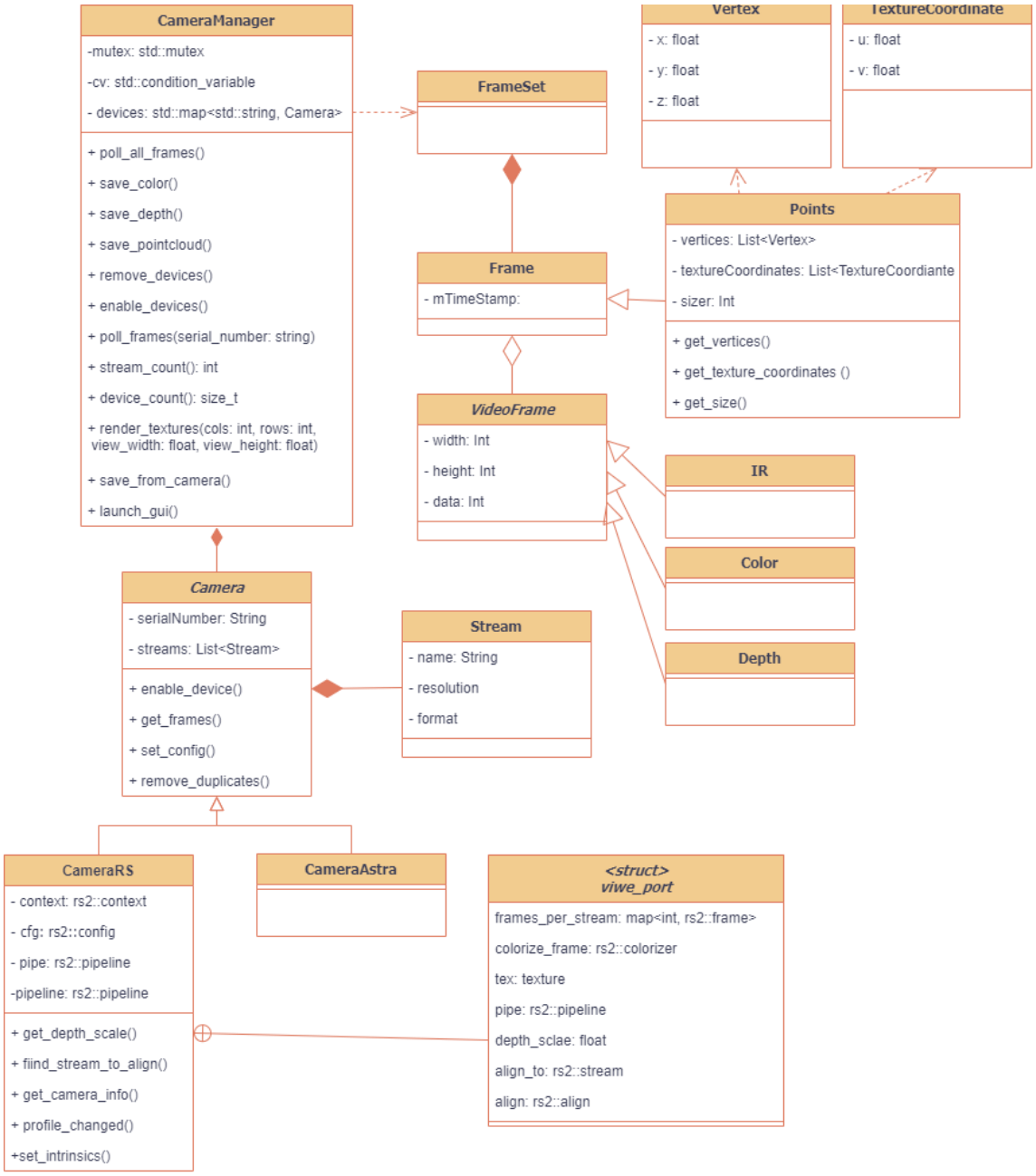

Figura 11. Diagrama de clases

- CameraManager.

  Esta clase es la que se encarga de la adquisición de imágenes de todos los sensores RGB-D que estén conectados al servidor, que se implementarán a través de una interfaz que se explicará a continuación.

- Camera.

  Interfaz que otorga al sistema la posibilidad de utilizar sensores RGBD de otras marcas, como el sensor Astra de Orbbec, haciendo que este tenga una mayor escalabilidad debido a que se puede tener desarrollado la implementación para los sensores Realsense y para los Astra. Además, contendrá un vector de clases Stream que abarcará los sensores específicos que se desean utilizar, que pueden ser: el de color, el de profundidad y el de infrarrojos.

- ViewPort.

  Estructura que facilita el control y manejo de las tuberías creadas para los dispositivos RGB-D, y así poder obtener toda la información necesaria cuando sea necesario.

- Frameset.

  Vector donde se almacenarán objetos de clase Frame, que es implementada por dos clases diferentes. Por un lado, la clase VideoFrame que guarda las adquisiciones de los sensores de color, profundidad e infrarrojo. Por otro lado, la clase Points que guarda los vértices de la nube de puntos y las coordenadas de textura. Finalmente, la clase Frameset corresponde a la adquisición que realiza la cámara, almacenando todos los datos de las capturas del objetivo que realiza el sensor.

2.2.2. Módulos y resultados

Puesto de manifiesto la estructura que va a tener el programa, se va a explicar brevemente la parte más importante del código, que son tanto la habilitación los sensores necesarios como la adquisición de datos para el funcionamiento del sistema.

En primer lugar, hay que habilitar todos los sensores que se necesitan para la adquisición de datos, siendo solo necesario obtener la información de los stream de color y de profundidad se debe proporcionar la configuración adecuada a los sensores. En segundo lugar, hay habilitar la cámara e iniciar las conexiones o tuberías por donde

obtendremos la información de estos streams. Por último, se añade toda la información de las cámaras asociadas a su número de serie, esto se realiza debido a que, posteriormente, se tiene que acceder a los datos de las cámaras. Como podemos apreciar en el siguiente código.

Código 2.1 Habilitar sensores

```
for (auto &&dev : ctx.query_devices()) // Query the list of
connected RealSense devices
            {
                  std::string
      serial_number(dev.get_info(RS2_CAMERA_INFO_SERIAL_NUMBER));
            std::lock_guard<std::mutex> lock(_mutex);
            if (_devices.find(serial_number) != _devices.end())
                return; //already in
            const std::shared_ptr<rs2_device> d = dev.get();
            const rs2_device *devi = d.get();

            // Start the pipeline with the configuration
            rs2::config cfg;
            cfg.enable_stream(RS2_STREAM_DEPTH, 0, WIDTH, HEIGHT,
RS2_FORMAT_Z16, FPS);
            cfg.enable_stream(RS2_STREAM_COLOR, 0, WIDTH, HEIGHT,
RS2_FORMAT_RGB8, FPS);
            cfg.enable_device(serial_number);
            rs2::pipeline pipe;
            rs2::pipeline_profile profile = pipe.start(cfg);
            float depth_scale =
get_depth_scale(profile.get_device());
            rs2_stream align_to =
find_stream_to_align(profile.get_streams());
            rs2::align align(align_to);
            _devices.emplace(serial_number, view_port{{}, {}, {},
pipe, profile, depth_scale, align_to, align});
            auto &&device = _devices.find(serial_number);
            // Capture 30 frames to give autoexposure, etc. a
chance to settle
            for (auto i = 0; i < 30; ++i)
             device->second.pipe.wait_for_frames();
            cont++;
        }
```

Después de configurar todos los sensores con los ajustes que se precisan para el buen funcionamiento del sistema, procedemos a la adquisición de imágenes y datos que necesarios, que son imagen de color, datos de profundidad por pixel y los datos de la nube de puntos del contorno del individuo.

En primer lugar, la imagen de color se guarda en un archivo con formato png. Para generar este archivo necesitamos: un archivo de imagen, el tamaño, los bytes por pixel, y los datos que conforman la imagen. Como cabe esperar, la información obtenida

corresponde a los ejes de coordenadas X e Y, siendo visible en el código 2.2 y en la figura que hay debajo (ver Figura 12).

Código 2.2 Captura imagen de color

```
void save_color(rs2::video_frame colorFrame, string serial)
{
    try
    {
        std::stringstream png_file;
        png_file << "Datos/" << serial << "-" <<
colorFrame.get_profile().stream_name() + "-" +
to_string(capture_count) << ".png";
        stbi_write_png(png_file.str().c_str(),
colorFrame.get_width(), colorFrame.get_height(),
                       colorFrame.get_bytes_per_pixel(),
colorFrame.get_data(), colorFrame.get_stride_in_bytes());
    }
}
```

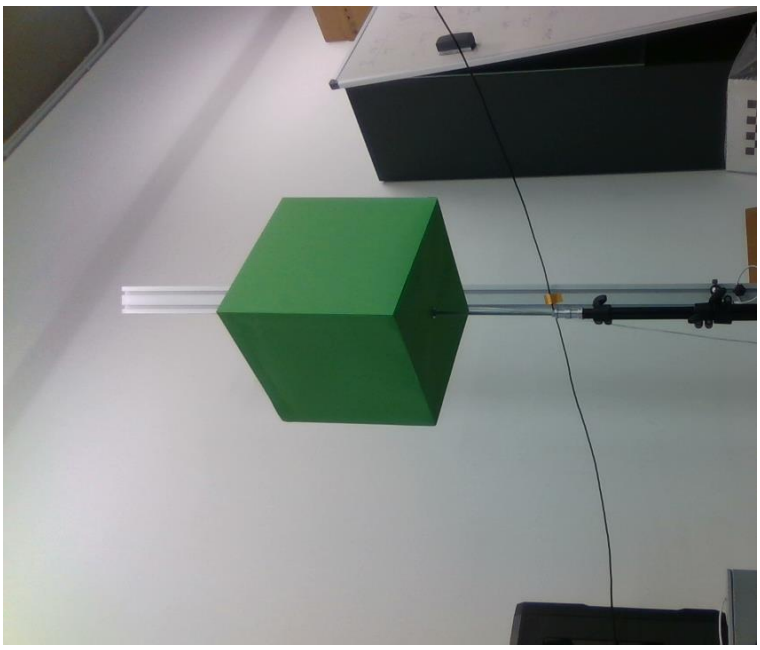

Figura 12. Imagen de color capturada con la cámara Realsense D435

En segundo lugar, los datos de profundidad se obtienen a partir de la distancia de cada pixel con respecto a la imagen de color, por lo que únicamente hay información de una de las tres coordenadas, la Z, esto es visible en el código 2.3. Se han realizado dos implementaciones que obtienen la información de profundidad que proporcionan los sensores en dos formatos diferentes, en texto y en imagen (ver figura 13).

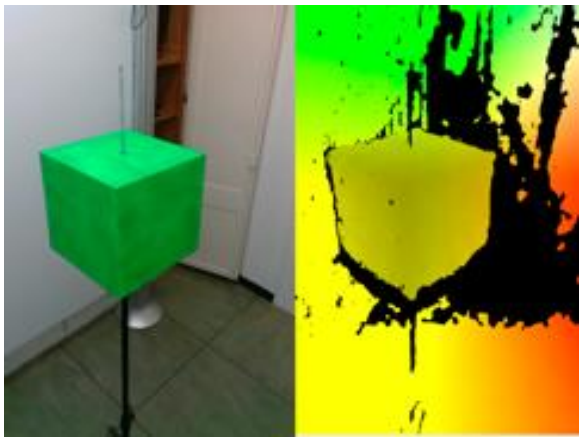

Figura 13. Imagen de color y de profundidad respectivamente

Como se ha expuesto previamente, hay dos formatos de obtener los datos de profundidad, y es el fichero de texto, el cual se necesita para el sistema de modelado. Esto es debido a que solo es necesario la información del eje de coordenadas Z, que representa la distancia entre el sensor y el objetivo que se enfoca en ese pixel (ver tabla 2). Por este motivo, se escribe la información utilizando dos bucles, como es visible en el código 2.3.

Código 2.3 Adquisición de datos de profundidad

```
void save_depth(rs2::depth_frame depthFrame, float
depth_scale, string serial)
{
        const uint16_t *p_depth_frame = reinterpret_cast<const
uint16_t *>(depthFrame.get_data());
        std::string name = "Datos/" + serial + "-" +
depthFrame.get_profile().stream_name() + "-" +
to_string(capture_count) + ".txt";
        std::ofstream fs(name);

        for (int y = 0; y < depthFrame.get_height(); y++)
       {
            auto depth_pixel_index = y *
depthFrame.get_width();
            for (int x = 0; x < depthFrame.get_width(); x++,
++depth_pixel_index)
            {
                auto pixels_distance = depth_scale *
p_depth_frame[depth_pixel_index];
                fs << pixels_distance << std::endl;
            }
```

Eje Z
1.941
1.941
1.941

Tabla 2. Muestra de datos de profundidad

Para finalizar, en lo que a implementación se refiere, se debe almacenar la nube de puntos en un fichero PLY. Esta información se guarda en un formato de coordenadas X, Y, Z y es truncada según el valor del eje Z, esto sirve para eliminar vértices que no son necesarios para la parte de modelación, como se puede apreciar en el código 2.4.

Código 2.4 Adquisición de nube de puntos

```
void save_pointCloudPLY(rs2::points points, string serial)
{
    auto v = points.get_vertices();
    std::string name = "Datos/" + serial + "-PointCloud-" +
to_string(capture_count) + ".ply";
    std::ofstream fs(name);
    fs << "ply\nformat ascii 1.0\ncomment VCGLIB generated\n";
    fs << "element vertex " << points.size() << std::endl;
    fs << "property float x\nproperty float y\nproperty float
z\n";
    fs << "end_header\n";
    for (int i = 0; i < points.size(); i++)
    {
        if (v[i].z > 4)
            fs << 0.0 << " " << 0.0 << " " << 0.0 << std::endl;
        else
            fs << v[i].x << " " << v[i].y << " " << v[i].z <<
std::endl;
    }
    fs.close();
}
```

Estos datos se visualizarán en formato de texto para, posteriormente, ser utilizados en el proceso de modelado (ver Tabla 3).

Eje X	Eje Y	Eje Z
-1.36512	-0.755033	1.941
-1.36301	-0.755033	1.941
-1.3609	-0.755033	1.941

Tabla 3. Información Nube de puntos 3 primeros pixeles

3. Seguridad y Protección de los datos

Como se exponía en el capítulo 1, en este proyecto se toman capturas del contorno de los pacientes para realizar estudios. Los datos obtenidos de los mismos tienen que ser salvaguardados especialmente, debido a su carácter personal.

En este capítulo se van a tratar las medidas de seguridad que se deben de aplicar en el proyecto para poder cumplir la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales y del Esquema Nacional de Seguridad.

3.1. Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales en el proyecto

Con el desarrollo del sistema de adquisición de imágenes 3D realizado, se debe tener en cuenta que el proyecto obtiene información privada de los pacientes que utilizan su servicio, por este motivo, esta información debe ser protegida y usada debidamente, amparado por el artículo 18.4 de la Constitución (Spain, 2018) y regulado por el Reglamento Europeo de Protección de Datos (RGPD en adelante). Además, hay que tener en cuenta que el proyecto está orientado en el ámbito médico y nutricional, de manera que, los datos pertenecientes a este ámbito están gozan de protección reforzada en dicha ley.

Debido a lo expuesto anteriormente, se ha realizado un estudio en el cual se detallan como tienen que ser usados estos datos y como deben ser protegidos para no recibir posibles sanciones por el uso indebido de esta información, lo cual mancharía la imagen del equipo de investigación y de la propia universidad.

3.2. Aspectos generales de la LOPDGDD

La Protección de Datos es un derecho fundamental recogido en el artículo 18.4 de la Constitución Española. Este derecho hace referencia al poder de disposición y control sobre los datos personales, el cual concede el derecho a las personas físicas para

consentir gestión de sus datos por terceros. De esta manera es la persona física la única facultada para decidir lo que se puede hacer con sus datos de carácter personal.

La LOPDGDD nace con el objetivo de garantizar y proteger el tratamiento de datos personales de un individuo identificable. En este marco, dicha ley, en sus artículos 7 y 8, hace referencia a este tipo de datos a fin de garantizar la protección jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos.

Cabe destacar que la RGPD declara que todo dato relativo a la salud del paciente debe ser especialmente protegido, esto provoca que se deban cumplir ciertos principios fundamentales para el tratamiento de la información del paciente conforme a la normativa, los cuales detallamos a continuación:

- Consentimiento.

  El titular tendrá que solicitar el consentimiento de los pacientes para poder tratar sus datos, salvo que nos encontremos en una de las excepciones que la Ley prevé.

  Este consentimiento, según la normativa europea, tendrá que ser explícito y recogido por escrito. En caso de que el paciente se menor de 14 años es necesario el consentimiento de los tutores legales en ese momento.

- Calidad de los datos.

  Sólo se podrán recoger datos de los pacientes cuando sean adecuados, pertinentes y no excesivos en relación con la finalidad para la cual hayan sido obtenidos.

  La finalidad debe ser determinada y se debe informar de la misma al paciente. Por lo tanto, es necesario realizar un estudio sobre las utilidades que se quieren dar a la información disponible, debido a que, en este proyecto la información obtenida es utilizada para realizar estudios sobre el funcionamiento del sistema, y es de carácter obligatorio informar previamente al paciente.

- Información.

  Se debe informar a los pacientes de:

- La existencia y finalidad de un fichero en el cual se añade su información personal.
- Los posibles destinatarios de la información de este fichero.
- Identidad y dirección del responsable del mantenimiento del mismo.
- Posibilidad del ejercicio de sus derechos.
- Confidencialidad.

Todas aquellas personas que tengan acceso a los datos de carácter personal, ya sea de pacientes o de trabajadores, están obligados al secreto profesional.

Además, hay que decir que la RGPD añade ciertas condiciones adicionales que se deben cumplir para poder tratar los datos conforme a la normativa. Dichas condiciones son las siguientes:

- Medidas organizativas y de seguridad.

  La nueva normativa prevé que las medidas de seguridad se apliquen en función del riesgo que pueda haber al tratar los datos. El tratamiento de datos de salud tiene un nivel de riesgo crítico, por lo que hay que diseñar una lista de medidas organizativas y de seguridad para salvaguardar el sistema de los posibles riesgos.

- Facilitar los derechos de acceso, rectificación, cancelación y oposición.

  Se debe informar a los pacientes que tienen la posibilidad de ejercer sus derechos, en cuanto a sus datos personales se refiere, de acceso, rectificación, cancelación y oposición.

  El procedimiento para el ejercicio de estos derechos debe hacerse siempre conforme a lo que marca la ley, ya que existen unos plazos y unas pautas tanto para ejercerlos como para facilitarlos.

- Evaluación de impacto.

  Es un análisis del riesgo de nuestro sistema, cuyo objetivo es permitir a los responsables del tratamiento tomar medidas adecuadas para reducir estos posibles riesgos.

- Registro de actividades de tratamiento.

Los responsables y los encargados están obligados a mantener un registro de las actividades de tratamiento que se hayan realizado.

Este registro debe contener los siguientes datos:

- Nombre y datos de contacto del responsable y, en su caso del corresponsable, representante del responsable y del delegado de protección de datos.
- Fines del tratamiento.
- Descripción de categorías de interesados y datos personales.
- Categorías de destinatarios existentes o previstos y las transferencias que se realicen.
- Plazos para la suspensión de datos, cuando sea posible.
- Descripción general de las medidas técnicas y organizativas de seguridad.

- Delegado de protección de datos.

  Se deberá contar con un delegado de protección de datos, ya que así lo exige la nueva normativa.

3.3. Tratamiento de los datos personales

Por lo que respecta al proyecto, se van a utilizar los datos personales de los pacientes de dos maneras:

- Seguimiento médico.
- Estudio del comportamiento del sistema desarrollado.

Dadas estas dos vertientes de uso de los datos personales de los pacientes, el proyecto debe cumplir las diversas disposiciones adicionales para el ámbito sanitario que se registran en el BOE, como, por ejemplo:

- El representante legal podrá otorgar el derecho para el uso de los datos del paciente con fines de investigación en salud.
- Las autoridades sanitarias e instituciones públicas con competencias en vigilancias de la salud publica podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

- Se considerará licita y compatible la reutilización de datos personales con fines de investigación en la materia de salud cuando, habiéndose obtenido el consentimiento para una finalidad.
- En estas circunstancias se debe publicar la información establecida por el artículo 13 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice el estudio clínico y notificar la existencia de esta información por los medios necesarios a los afectados.
- Se considera lícito el uso de datos personales seudonimizados con finos de investigación en salud. Para poder utilizar este tipo de datos se requiere que se pueda enlazar los datos seudonimizados con los datos reales posibilitando la reidentificación y que el equipo de investigación sea el único que tiene acceso a estos datos. En cualquier caso, se podrá proceder a una reidentificación cuando se aprecie la existencia de un peligro para la salud de una persona, o incluso una amenaza grave para sus derechos o para asegurar una adecuada asistencia sanitaria. Además, destacar que la investigación debe tener un objetivo público relacionado con la seguridad del Estado y pública. Por último, se debe añadir a la evaluación de impacto los riesgos de reidentificación vinculados a la seudonimización de los datos.
- El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial

3.4. Aplicación del Esquema Nacional de Seguridad

Toda la información que se obtiene en el proyecto ha de ser protegida en nuestros sistemas informáticos, pero además es necesario proteger de cualquier riesgo que podamos tener y que puedan afectar tanto a la disponibilidad del sistema como al funcionamiento del mismo, para esto hay que basarse en la información recogida en la Guía de Implantación del ENS publicada por el Centro de Criptografía Nacional (CCN-STIC, 2017). Este esquema es de obligatorio cumplimiento para el conjunto de la

administración española y debe ser aplicado a todos los sistemas, datos, comunicaciones y servicios electrónicos de la administración.

Esta seguridad que se debe implementar tiene como finalidad que el proyecto pueda cumplir con sus objetivos utilizando sistemas de la información. Para que esto suceda, hay que tener en cuenta una serie de principios básicos antes de tomar decisiones, las cuales son:

- Seguridad Integral.

  En la gestión de seguridad hay que considerar los elementos técnicos, humanos, materiales y organizativos que estén relacionados con el sistema, convirtiendo esto en un proceso integral. Hay que tener en cuenta que hay que formar y concienciar al personal que tenga alguna responsabilidad en los servicios electrónicos para intentar prevenir los errores humanos.
- Gestión de Riesgos.

  Para reducir los posibles riesgos debemos utilizar el análisis y la gestión de los mismos. En la parte de análisis de riesgos se detectarán los problemas de seguridad y, posteriormente, se categorizarán, mientras que con la gestión se reducirán los riesgos a un nivel aceptable.
- Prevención, reacción y recuperación.

  Se deben tomar diferentes medidas para afrontar los posibles riesgos que estén presentes en el proyecto, por lo que se tienen que crear medidas de prevención, detección y recuperación. La utilización de estos tipos de medidas dará un enfoque integral a la seguridad evitando incidencias y reduciendo el impacto de estas.
- Líneas de defensa.

  El sistema debe contar con sucesivas capas de protección de manera que un incidente no sea capaz de desarrollar todo su potencial dañino en caso de que ocurra.
- Reevaluación periódica.

  Revisión de las medidas de seguridad para verificar si siguen siendo adecuadas a los riesgos detectados y que mantienen su eficacia protegiendo el sistema contra ellos.
- Función diferenciada.

  El ENS estipula que las funciones de responsable de la información, responsable del servicio y responsable de la seguridad deben estar

separadas y serán estos los que definan los requisitos de seguridad de cada tipo.

3.5. Plan de Adecuación

El Plan de Adecuación es el punto de partida para abordar el proceso de implantación del ENS y está compuesto por las siguientes actuaciones:

- Política de Seguridad.
- Información que maneja.
- Servicios que se presentan.
- Datos de carácter personal.
- Categoría del sistema.
- Declaración de aplicabilidad.
- Análisis de riesgos.
- Insuficiencia del sistema.
- Plan de mejora continua de la seguridad.

Este plan debe ser desarrollado por el responsable de seguridad o la persona que desempeñe esta función de forma temporal durante en el proyecto. A continuación, se explican todos los puntos que se han comentado anteriormente.

- Política de Seguridad.

  La política de seguridad se debe desarrollar teniendo en cuenta los principios básicos y en base a los requisitos mínimos de seguridad establecidos por la normativa del ENS, como se exige en el Anexo II del Real Decreto ENS.

  Pero de no ser así, el plan tendrá que recoger la planificación de la modificación de la política de seguridad existente o el desarrollo de una nueva que cumpla con todos los requisitos.
- Información que maneja.

  Se deberá inventariar y valorar la información que vamos a manejar, junto con una justificación y la categorización del sistema, como se establece en el anexo I del Real Decreto ENS.

  En el caso de que no haber una política de seguridad clara y definida, podría causar problemas en el momento de llevar a cabo el inventario de toda la

información utilizada, por lo que el responsable de seguridad tendrá que realizar la valoración provisional de toda la información, dejando constancia de los motivos y razonamientos para determinar las valoraciones documentadas.

- Servicios que se prestan.

  En la misma línea que el apartado anterior, se debe valorar e inventariar los servicios que se prestan según lo establecido en el Anexo I del ENS.

  Puede darse el caso de que la política de seguridad sea insuficiente, por lo que el responsable de seguridad será el encargado de realizar una valoración provisional junto con la motivación y razonamiento de esta valoración.

- Datos de carácter personal.

  Cuando el sistema maneja información de carácter personal, se debe incluir la relación de dicha información en el plan de adecuación.

- Categoría del sistema.

  Junto con las valoraciones que se han descrito anteriormente de la información que se maneja y de los servicios prestados el responsable de seguridad se debe encargar de establecer la categoría del sistema siguiendo los criterios y pasos recogidos en el anexo I del ENS.

  Tanto los servicios como la información se deben valorar en función de la importancia de cada uno de los criterios de valoración. Estos criterios se describen brevemente a continuación.

    - Disponibilidad. Se tendrá acceso al servicio y a la información cuando se requiera.
    - Integridad. La información del sistema no debe ser alterada de manera no autorizada.
    - Confidencialidad. La información no se difunde a entidades o procesos no autorizados.
    - Trazabilidad. Las acciones que se realizan en la información tienen que conocerse.
    - Autenticidad. Garantizar la fuente de donde proceden los datos.

  Por otro lado, se pueden dividir los sistemas en subsistemas de ser posible, lo cual nos permitirá aplicar las medidas de seguridad exigidas para niveles altos a aquellos segmentos que lo requieran, y no a todo el sistema.

Por último, el nivel del sistema de cada dimensión será el mayor de los establecidos para cada servicio e información, el criterio para valorar cada una de estas pautas utiliza una escala de tres puntos: bajo, medio y alto.

- Análisis de riesgos.

  El análisis de riesgos debe permitir identificar y priorizar los riesgos más significativos a fin de conocer, a cuál de ellos estamos sometidos y tomar las medidas o técnicas oportunas para combatir los mismos.

  Para realizar el análisis de riesgos se debe partir de un inventario de todos los activos de los servicios de administración electrónica, como pueden ser el hardware, software, personal e instalaciones.

  Estos activos reciben la valoración de los servicios e información que dependen de ellos.

  Tras esta valoración de los activos se deben valorar las amenazas que les pueden afectar y con qué frecuencia ocurren. Con estos datos, se obtendrá un informe de las diferentes amenazas, vulnerabilidades e impactos que podrían producirse en los sistemas de información. Con esto se consigue una valoración del riesgo potencial de los activos en caso de no estar protegidos.

  Posteriormente, se valorará la madurez de las medidas implantadas para proteger los activos, para esta valoración hay 5 niveles:

Nivel	Significado	Descripción
n.a.	No es aplicable	
L0	Inexistente	En el nivel L0 de madurez no se implantan medidas.
L1	Inicial/ad hoc	Las medidas de seguridad existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las entidades exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del este nivel depende de tener personal de alta calidad
L2	Reproducible, pero intuitivo	La eficacia de las medidas de seguridad depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son

		repetibles, pero no hay plan para los incidentes más allá de la reacción a los hechos.
L3	Proceso definido	Se despliegan y se gestionan las medidas de seguridad. Hay una normativa establecida y ciertos procedimientos para garantizar la reacción profesional ante los incidentes y se ejerce un mantenimiento regular de las protecciones, obteniendo altas posibilidades de sobrevivir, aunque siempre queda el factor de lo no planificado.
L4	Gestionado y medible	En este nivel el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa mientras que en el nivel L3 era únicamente cualitativa.
L5	Optimizado	Este nivel se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras por lo que se establecen objetivos cuantitativos de mejoras de procesos y se revisan continuamente.

Tabla 4. Niveles de madurez

Para este análisis la metodología utilizada es MARGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información del Ministerio de Administraciones Públicas.

Esta metodología propone una serie de amenazas que afectan a los activos de proyecto pudiendo degradar el valor de estos, por lo que para gestionar los riesgos se hacen uso de las salvaguardas para hacer frente a las amenazas y mitigar el impacto que causan en el proyecto.

La herramienta con la que se implementa esta metodología es PILAR, que soporta el análisis y tratamiento de riesgos de un sistema informático siguiendo la metodología MARGERIT.

- Declaración de aplicabilidad.

  Observando los requerimientos del anexo II del ENS y los requerimientos derivados de los datos personales, el responsable de seguridad documentará una lista de medidas aplicables al sistema.

- Insuficiencias del sistema.

  Hay que identificar las carencias en el actual sistema de gestión de seguridad de la información y documentarlo. Estas carencias se pueden detectar en varios aspectos:

  - Desviaciones de lo exigido en el Anexo II para valorar el sistema y seleccionar las medidas de seguridad pertinentes.
  - Incumplimientos de los requisitos exigidos por el Real Decreto del ENS para los datos de carácter personal tratados por el sistema.
  - Existencia de riesgos que no son aceptables por el proyecto.

  Los riesgos residuales debes ser aceptados por los demás responsables, pero en el caso de que no haya responsable o la aceptación del riesgo no sea formal, será el responsable de seguridad el que tome la decisión indicando porque acepta o no estos riesgos residuales.

- Plan de mejora de la seguridad.

  Partiendo de toda la información recopilada y teniendo en cuenta las carencias detectadas se elaborará un plan de mejora de la seguridad que detallará las acciones que se deben tomar para subsanarlas, por lo que habrá que documentar la siguiente información:

  - La insuficiencia subsanada.
  - El plazo previsto de ejecución, indicando fecha de inicio y fecha de finalización.
  - Los hitos del proyecto.
  - Una estimación del coste que supone.

3.6. Implantación del Plan de Adecuación en el proyecto Tech4Diet

En este apartado se implementará el plan de adecuación explicado en el punto anterior. Este desarrollo permitirá al proyecto tener un documento donde especifique que medidas de seguridad se deben implementar.

3.6.1. Contexto

Nada más acabar el desarrollo de parte de los sistemas en los que se centran el proyecto Tech4Diet se decidió tomar las medidas de seguridad necesarias para proteger toda la información que posteriormente obtenida, ya sea de los pacientes, de los individuos que participan en el proyecto, o de la información relativa del proyecto.

Existe un grupo de informática, formado principalmente por 4 personas, en el cual no hay un responsable de Seguridad definido. El grupo trabaja en los laboratorios de informática de la Universidad de Alicante, por lo que el CPD se encontrará en los servidores de la misma.

En la fase de experimentación del proyecto se pondrán en funcionamiento diferentes servicios, acceso a los datos médicos de los pacientes desde la página web, acceso a los datos médicos de los pacientes desde la aplicación móvil, portal web, además del servicio de captura y modelado de los datos.

Las aplicaciones utilizadas son:

- Tech4DietAM. Para la adquisición y almacenamiento de datos de diferente índole, como dato de profundidad, imágenes a color o nube de puntos de la estructura corporal del sujeto o paciente, y posteriormente estos datos se transforman en una imagen 3D en una fase de modelado.
- Tech4Diet3D. Para la visualización de los datos médicos del paciente, por parte de este, con la tecnología de realidad virtual desde el móvil.
- Tech4DietDesktop. Para la visualización de los datos médicos del paciente, por parte de este, desde una aplicación de escritorio.
- Portal Web. Página web del proyecto donde se subirán noticias en cuanto al proyecto, información de contacto, publicaciones, etc.

El mapa de red del proyecto quedaría como en la siguiente figura (ver Figura 14).

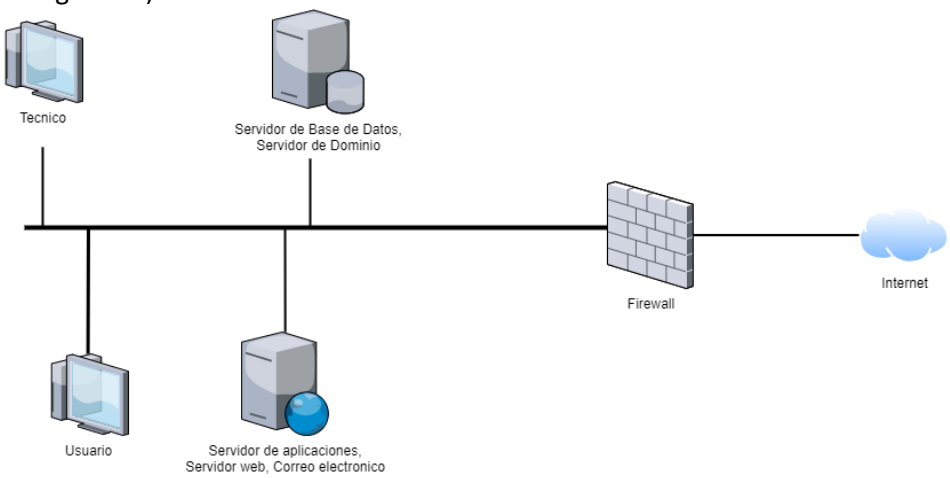

Figura 14. Mapa de Red de Tech4Diet

3.6.2. Política de Seguridad

3.6.2.1. *Introducción*

El proyecto depende completamente de los sistemas TIC (Tecnologías de Información y Comunicaciones) para cumplir con sus objetivos. Estos sistemas deben ser administrados con cautela, tomando las medidas adecuadas para protegerlos de posibles daños accidentales o de confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación de los servicios de manera continuada, actuando preventivamente, supervisando la actividad diaria y reaccionando con rapidez a los incidentes que sucedan a lo largo de la vida útil del sistema.

Los sistemas TIC deben estar protegidos contra amenazas con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso y valor de la información y los servicios. Para defenderse de las posibles amenazas, se requiere una estrategia que se adapte a los cambios para garantizar la prestación continua de los servicios. Esto implica que el en el proyecto se deben aplicar las medidas mínimas de seguridad exigidas por el ENS, así como seguir y analizar las prestaciones del servicio, las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios.

3.6.2.2. *Prevención*

Tech4Diet intenta prevenir que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se debe implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control de amenazas y riesgos gracias a la realización de evaluaciones. Estos controles, los roles y las responsabilidades del personal, deben estar definidos y documentados.

Para garantizar el cumplimiento de la política, la entidad:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.6.2.3. *Detección*

Se deben monitorizar de manera continua las prestaciones de los servicios para detectar y actuar ante posibles anomalías como se describe en el artículo 9 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que llegue a los responsables y cuando se produce una desviación significativa de los parámetros preestablecido como normales.

3.6.2.4. *Respuesta*

El proyecto debe cumplir los siguientes puntos para tener un sistema de respuesta eficiente ante los incidentes:

- Establecer mecanismos de seguridad para responder a los posibles incidentes.

- Se debe designar un punto de contacto para las comunicaciones relacionadas con los incidentes detectados dentro del área del proyecto.
- Establecer protocolos para el intercambio de información que tenga relación con el incidente. Además, se debe comunicar con los Equipos de Respuesta a Emergencias (CERT) reconocidos a nivel nacional.

3.6.2.5. *Recuperación*

Se deben desarrollar planes de continuidad de los sistemas TI para poder garantizar la disponibilidad de los servicios críticos, esto debe ser parte del plan de continuidad de negocio y actividades de recuperación del proyecto.

3.6.2.6. *Misión*

Como proyecto perteneciente a la Universidad de Alicante, la misión tiene una línea similar a de la propia Universidad que son el compromiso con el avance y la mejora de la sociedad mediante la creación de conocimiento y del desarrollo cultural, científico y tecnológico.

Mas centrado a la línea del proyecto, junto con los puntos anteriores, hay que añadir que es necesario una infraestructura TI para conseguir funciones necesarias para la consecución de los objetivos principales.

3.6.2.7. *Alcance*

El proyecto considera necesaria la aplicación de la presente política de seguridad sobre todo el conjunto de los sistemas informáticos de la universidad.

3.6.2.8. *Marco Normativo*

Esta política se enmarca en el marco jurídico definido por las leyes y Reales Decretos siguientes:

- Ley Orgánica de Universidades (6/2001) y Ley Orgánica de modificación de la L.O.U. (4/2007).
- Esquema Nacional de Seguridad (39/2015).

- Ley de acceso electrónico de los ciudadanos a los servicios públicos (11/2007).
- Ley de Protección de Datos Personales y garantía de los derechos digitales (3/2018).
- Ley de Servicios de la Sociedad de la información (34/2002).

3.6.2.9. *Datos de carácter personal*

El proyecto realiza tratamientos en los que hace uso de datos de carácter personal. Todos los sistemas de información se ajustarán a los niveles mínimos de seguridad requeridos por la LOPDGDD para la naturaleza y finalidad de los datos de carácter personal procedente de la normativa aplicada en la Universidad de Alicante.

3.6.2.10. *Gestión de Riesgos*

Todos los sistemas afectados por esta política de seguridad deben estar sujetos a un análisis de riesgos, evaluando las amenazas a las que están expuestos. Este análisis se repetirá después de que suceda una de las siguientes situaciones: que haya pasado un año desde la última revisión, cuando cambien la información que se utiliza, que suceda un incidente grave o que se detecten vulnerabilidades.

3.6.2.11. *Obligaciones del personal*

Todos los miembros del proyecto tienen la obligación de conocer y cumplir esta política de seguridad y la normativa de seguridad desarrollada a partir de ella.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el empleo seguro de los sistemas en la medida en que lo necesiten para realizar su trabajo.

3.6.3. Categorización del sistema

Se ha realizado una propuesta de valoración inicial de los activos de Servicios e Información. En esta valoración se ha tomado en consideración la naturaleza de cada uno y la normativa que pudiera serle de aplicación.

Para valorar estos servicios, se ha tenido en cuenta:

- Que estos disponen de requisitos relevantes en términos de Disponibilidad (D).
- Que los requisitos de Confidencialidad (C), Integridad (I), Autenticidad (A) y Trazabilidad (T) se heredarán de los de la información asociada al servicio correspondiente.
- Cuando un aspecto no requiere medidas de seguridad se indicará con la valoración "Sin valorar" (S). En caso de que se necesite alguna medida de seguridad se indicará con 3 tipos diferentes de valoración según corresponda: "Perjuicio muy grave" (A), "prejuicio grave" (M) y "prejuicio limitado" (B), según estos tipos.

ID	Activo	C	I	A	T	D
	Servicio					
S 01	Portal Web	-	-	-	-	B
S 02	Salud	-	-	-	-	M

Tabla 5. Valoración de Servicios

3.6.3.1. *Justificación de la valoración de los servicios*

La valoración se ha realizado en base a las consecuencias que tendría un incidente de seguridad en la parte de Disponibilidad, determinando las posibles consecuencias de un incidente que impida que una persona con autorización pueda acceder al servicio, como:

Valoración de los servicios		D
Sin Valorar	Cuando la información es prescindible por tiempo indefinido	
Capacidad	Perjuicio muy grave La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	
	Perjuicio grave Reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose	X

	Perjuicio limitado Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	X
Daño Activo	Perjuicio muy grave El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado El sufrimiento de un daño menor por los activos de la organización	X
Cumplimiento Servicio	Perjuicio muy grave Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
Cumplimiento ley	Perjuicio muy grave El incumplimiento grave de alguna ley o regulación	
	Perjuicio grave El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	X
	Perjuicio limitado El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
Ciudadanía	Perjuicio muy grave Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave Causar un perjuicio significativo a algún individuo, de difícil reparación	X

	Perjuicio limitado Causar un perjuicio menor a algún individuo, que, aun siendo molesto, pueda ser fácilmente reparable	X
Tiempo de Recuperación de Servicio (RTO)	Prejuicio muy grave RTO < 4 horas	
	Prejuicio grave 4 horas < RTO < 1 día	X
	Perjuicio limitado 1 día < RTO < 5 días	X

Tabla 6. Parámetros de valoración para la disponibilidad del sistema

Para valorar la información se ha considerado que:

- Que la información impone requisitos relevantes de los términos Confidencialidad (C), Integridad (I), Autenticidad (A) y Trazabilidad (T), estos se asocian a los Servicios que la tratan.
- El nivel de seguridad requerido en el aspecto de Confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.
- El nivel de seguridad requerido en el aspecto de Integridad se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.
- El nivel de seguridad requerido en el aspecto de Autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.
- El nivel de seguridad requerido en el aspecto de Trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear, a posteriori, quién ha accedido, o modificado, cierta información.

ID	Activo	C	I	A	T	D
	Información					
I 01	Información Web	B	B	B	B	-
I 02	Gestión de Datos de carácter personal	A	M	M	A	-

Tabla 7. Valoración de la información

3.6.3.2. *Justificación de la valoración de la información.*

La justificación de la valoración otorgada en cada uno de los términos afectados se ha realizado en base a las consecuencias que tendría un incidente de seguridad, siendo la expuesta a continuación.

Se ha determinado las posibles consecuencias de un incidente en el término de Confidencialidad que permita que la información sea rebelada a persona o que no necesitan conocer la información (ver Tabla 8).

Valoración de los servicios		C
Sin Valorar	Cuando la información es prescindible por tiempo indefinido	
Capacidad	Perjuicio muy grave La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	X
	Perjuicio grave Reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose	
	Perjuicio limitado Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	
Daño Activo	Perjuicio muy grave El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	X
	Perjuicio grave El sufrimiento de un daño significativo por los activos de la organización	

	Perjuicio limitado El sufrimiento de un daño menor por los activos de la organización	X
Cumplimiento Servicio	Perjuicio muy grave Anulada la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio grave Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio limitado Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
Cumplimiento ley	Perjuicio muy grave El incumplimiento grave de alguna ley o regulación	X
	Perjuicio grave El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	
	Perjuicio limitado El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
Ciudadanía	Perjuicio muy grave Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	X
	Perjuicio grave Causar un perjuicio significativo a algún individuo, de difícil reparación	
	Perjuicio limitado Causar un perjuicio menor a algún individuo, que, aun siendo molesto, pueda ser fácilmente reparable	X

Tabla 8. Parámetros de valoración para la confidencialidad del sistema

Se ha determinado las posibles consecuencias de un incidente en el término de Integridad que permita que la información sea modifica por una persona que no está autorizada (ver Tabla 9).

Valoración de los servicios		I
Sin Valorar	Cuando la información es prescindible por tiempo indefinido.	
Capacidad	Perjuicio muy grave. La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.	
	Perjuicio grave. Reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.	X
	Perjuicio limitado Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	X
Daño Activo	Perjuicio muy grave El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave El sufrimiento de un daño significativo por los activos de la organización	X
	Perjuicio limitado El sufrimiento de un daño menor por los activos de la organización	X
Cumplimiento Servicio	Perjuicio muy grave Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
Cumplimiento ley	Perjuicio muy grave El incumplimiento grave de alguna ley o regulación	
	Perjuicio grave El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	X

	Perjuicio limitado El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
Ciudadanía	Perjuicio muy grave Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave Causar un perjuicio significativo a algún individuo, de difícil reparación	X
	Perjuicio limitado Causar un perjuicio menor a algún individuo, que, aun siendo molesto, pueda ser fácilmente reparable	X

Tabla 9. Parámetros de valoración para la integridad del sistema

Se ha determinado las posibles consecuencias de un incidente en el término de Autenticidad provocando que esta no sea autentica (ver Tabla 10).

Valoración de los servicios		A
Sin Valorar	Cuando la información es prescindible por tiempo indefinido	
Capacidad	Perjuicio muy grave La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	
	Perjuicio grave Reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose	X
	Perjuicio limitado Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	X
Daño Activo	Perjuicio muy grave El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	
	Perjuicio grave El sufrimiento de un daño significativo por los activos de la organización	X

	Perjuicio limitado El sufrimiento de un daño menor por los activos de la organización	X
Cumplimiento Servicio	Perjuicio muy grave Anulada la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio grave Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio limitado Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
Cumplimiento ley	Perjuicio muy grave El incumplimiento grave de alguna ley o regulación	
	Perjuicio grave El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	X
	Perjuicio limitado El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
Ciudadanía	Perjuicio muy grave Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	
	Perjuicio grave Causar un perjuicio significativo a algún individuo, de difícil reparación	X
	Perjuicio limitado Causar un perjuicio menor a algún individuo, que, aun siendo molesto, pueda ser fácilmente reparable	X

Tabla 10. Parámetros de valoración para la autenticidad del sistema

Se ha determinado las posibles consecuencias de un incidente en el término de Trazabilidad impidiendo que se pueda rastrear quien ha accedido o modificado cierta información (ver Tabla 11).

Valoración de los servicios		T
Sin Valorar	Cuando la información es prescindible por tiempo indefinido	
Capacidad	Perjuicio muy grave La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose	X
	Perjuicio grave Reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose	
	Perjuicio limitado Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	X
Daño Activo	Perjuicio muy grave El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.	X
	Perjuicio grave El sufrimiento de un daño significativo por los activos de la organización	
	Perjuicio limitado El sufrimiento de un daño menor por los activos de la organización	X
Cumplimiento Servicio	Perjuicio muy grave Anulada la capacidad para cumplir con las obligaciones diarias del servicio	X
	Perjuicio grave Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	
	Perjuicio limitado Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	X
Cumplimiento ley	Perjuicio muy grave El incumplimiento grave de alguna ley o regulación	X
	Perjuicio grave El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	

	Perjuicio limitado El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	X
Ciudadanía	Perjuicio muy grave Causar un perjuicio grave a algún individuo, de difícil o imposible reparación	X
	Perjuicio grave Causar un perjuicio significativo a algún individuo, de difícil reparación	
	Perjuicio limitado Causar un perjuicio menor a algún individuo, que, aun siendo molesto, pueda ser fácilmente reparable	X

Tabla 11. Parámetros de valoración para la trazabilidad del sistema

Por último, después de revisar la categorización de los servicios y de la información, podemos asegurar que la categoría del sistema es Alta, como se establece al determinar los niveles máximos alcanzados para cada termino.

3.6.4. Valoración de los activos

Aquí se valoran el resto de los activos que no pertenecen a las categorías de servicio e información, pero mantienen dependencias con estas.

Para esto, se han identificados las dependencias entre los activos de hardware, software, personal e instalaciones con los activos que pertenecen a las categorías de servicio e información (ver Tablas 12).

ID	Activos	Portal Web	Salud	Información Web	Gestión de Datos de carácter personal
	Hardware				
	Servidor Web	X	X	X	X
	Equipos de usuario	X	X	X	X
	Periféricos		X		
	Servidor de Base de datos	X	X	X	X
	Software				

	Portal Web	X		X	
	Tech4DietAM		X		X
	Tech4Diet3D		X		X
	Tech4DietDesktop		X		X
	Personal				
	Personal Técnico	X	X	X	X
	Personal Medico		X	X	X
	Instalaciones				
	Laboratorio Universitario	X	X	X	X

Tabla 12.Dependencias de los activos

La valoración de estos activos según especifica el ENS, es la heredada de los activos de tipo de servicio e información. En consecuencia, su valoración, teniendo en cuenta las dependencias identificadas, es la siguiente (ver Tabla 13).

ID	Activos	C	I	A	T	D
	Hardware					
HW 01	Servidor Web	A	M	M	A	M
HW 02	Equipos de usuario	A	M	M	A	M
HW 03	Periféricos	A	M	M	A	M
HW 04	Servidor de Base de datos	A	M	M	A	M
	Software					
SW 01	Portal Web	B	B	B	B	B
SW 02	Tech4DietAM	A	M	M	A	M
SW 03	Tech4Diet3D	A	M	M	A	M
SW 04	Tech4DietDesktop	A	M	M	A	M
	Personal					
P 01	Personal Técnico	A	M	M	A	M
P 02	Personal Medico	A	M	M	A	M
	Instalaciones					
IN 01	Laboratorio Universitario	A	M	M	A	M

Tabla 13. Valoración de los activos

3.6.5. Análisis de Riesgos con PILAR

Ya identificados los activos que pertenecen a los servicios y a la información de dichos servicios se debe evaluar mediante la herramienta PILAR. Se introducen los datos recogidos previamente y obtenemos los riesgos potenciales y el riesgo actual, estos dos hacen referencia a los riesgos que habría sin aplicar medidas de seguridad, y el segundo, con las medidas de seguridad en el nivel actual.

PILAR estima los riesgos según una escala simple con los siguientes valores (ver figura 15).

Figura 15. Escala de estimación de Riesgos

Así mismo, PILAR añade un decimal para presentar los niveles de criticidad para poder relativizar el riesgo dentro de un mismo nivel.

- Análisis de riesgos potencial:

potencial | current | target | ENS

	activo	[D]	[I]	[C]	[A]	[T]
	ACTIVOS	{4,2}	{3,7}	{5,1}	{3,3}	{5,7}
	[S01] Portal Web	{1,9}				
	[D] disponibilidad	{1,9}				
	[S02] SALUD	{4,2}				
	[D] disponibilidad	{4,2}				
	[I01] Informacion Web		{1,9}	{1,5}	{1,5}	{2,2}
	[I] integridad de los datos		{1,9}			
	[C] confidencialidad de los datos			{1,5}		
	[A] autenticidad de los usuarios y de la información				{1,5}	
	[T] trazabilidad del servicio y de los datos					{2,2}
	[I02] Gestion de Datos de Caracter peronal		{3,7}	{5,1}	{3,3}	{5,7}
	[I] integridad de los datos		{3,7}			
	[C] confidencialidad de los datos			{5,1}		
	[A] autenticidad de los usuarios y de la información				{3,3}	
	[T] trazabilidad del servicio y de los datos					{5,7}

Figura 16. Análisis del Riesgo potencial por Pilar

- Análisis de riesgos actual:

potencial | current | target | ENS

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{3,6}	{3,0}	{4,4}	{2,7}	{5,0}
[S01] Portal Web	{1,2}				
[D] disponibilidad	{1,2}				
[S02] SALUD	{3,6}				
[D] disponibilidad	{3,6}				
[I01] Informacion Web		{1,2}	{0,98}	{0,98}	{1,5}
[I] integridad de los datos		{1,2}			
[C] confidencialidad de los datos			{0,98}		
[A] autenticidad de los usuarios y de la información				{0,98}	
[T] trazabilidad del servicio y de los datos					{1,5}
[I02] Gestion de Datos de Caracter peronal		{3,0}	{4,4}	{2,7}	{5,0}
[I] integridad de los datos		{3,0}			
[C] confidencialidad de los datos			{4,4}		
[A] autenticidad de los usuarios y de la información				{2,7}	
[T] trazabilidad del servicio y de los datos					{5,0}

Figura 17. Análisis del riesgo actual

3.6.6. Declaración de aplicabilidad

Teniendo en cuenta que la categorización del sistema del proyecto es alta y los resultados del análisis de Riesgo, PILAR nos ofrece a través de su programa cuales son las medidas que debemos aplicar (ver Figura 18).

control	...	aplica
[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)		
[org] Marco organizativo		M
[org.1] Política de Seguridad		M
[org.2] Normativa de seguridad		M
[org.3] Procedimientos de seguridad		M
[org.4] Proceso de autorización		M
[op] Marco operacional		M
[op.pl] Planificación		M
[op.acc] Control de acceso		M
[op.exp] Explotación		M
[op.ext] Servicios externos		
[op.cont] Continuidad del servicio		M
[op.mon] Monitorización del sistema		M
[mp] Medidas de protección		M
[mp.if] Protección de las instalaciones e infraestructuras		
[mp.per] Gestión del personal		
[mp.eq] Protección de los equipos		M
[mp.com] Protección de las comunicaciones		M
[mp.si] Protección de los soportes de información		
[mp.sw] Protección de las aplicaciones informáticas (SW)		M
[mp.info] Protección de la información		
[mp.s] Protección de los servicios		M

Figura 18. Medidas que aplicar en el proyecto

Además, la herramienta genera un documento con unas tablas que amplían las medidas que se deben aplicar, como podemos ver en las siguientes tablas:

[org] Marco organizativo

control	aplica
[org] Marco organizativo	obligatorio
[org.1] Política de Seguridad	obligatorio
[org.2] Normativa de seguridad	obligatorio
[org.3] Procedimientos de seguridad	obligatorio
[org.4] Proceso de autorización	obligatorio

Tabla 14. Marco Organizativo

[op] Marco operacional

control	aplica
[op] Marco operacional	obligatorio
[op.pl] Planificación	obligatorio
[op.pl.1] Análisis de riesgos	obligatorio
[op.pl.2] Arquitectura de seguridad	obligatorio
[op.pl.3] Adquisición de nuevos componentes	obligatorio
[op.pl.4] Dimensionamiento / Gestión de capacidades	obligatorio
[op.pl.5] Componentes certificados	obligatorio

Tabla 15. Planificación

control	aplica
[op] Marco operacional	obligatorio
[op.acc] Control de acceso	obligatorio
[op.acc.1] Identificación	obligatorio
[op.acc.2] Requisitos de acceso	obligatorio

[op.acc.3] Segregación de funciones y tareas	obligatorio
[op.acc.4] Proceso de gestión de derechos de acceso	obligatorio
[op.acc.5] Mecanismo de autenticación	obligatorio
[op.acc.6] Acceso local	obligatorio
[op.acc.7] Acceso remoto	obligatorio

Tabla 16. Control de acceso

control	**aplica**
[op] Marco operacional	obligatorio
[op.exp] Explotación	obligatorio
[op.exp.1] Inventario de activos	obligatorio
[op.exp.2] Configuración de seguridad	obligatorio
[op.exp.3] Gestión de la configuración	obligatorio
[op.exp.4] Mantenimiento	obligatorio
[op.exp.5] Gestión de cambios	obligatorio
[op.exp.6] Protección frente a código dañino	obligatorio
[op.exp.7] Gestión de incidentes	obligatorio
[op.exp.8] Registro de la actividad de los usuarios	obligatorio
[op.exp.9] Registro de la gestión de incidentes	obligatorio
[op.exp.10] Protección de los registros de actividad	obligatorio
[op.exp.11] Protección de claves criptográficas	sí

Tabla 17.Explotación

control	aplica
[op] Marco operacional	obligatorio
[op.ext] Servicios externos	sí
[op.ext.1] Contratación y acuerdos de nivel de servicio	sí
[op.ext.2] Gestión diaria	sí
[op.ext.9] Medios alternativos	sí

Tabla 18. Servicios externos

control	aplica
[op] Marco operacional	obligatorio
[op.cont] Continuidad del servicio	obligatorio
[op.cont.1] Análisis de impacto	obligatorio
[op.cont.2] Plan de continuidad	sí
[op.cont.3] Pruebas periódicas	sí

Tabla 19. Continuidad del servicio

control	aplica
[op] Marco operacional	obligatorio
[op.mon] Monitorización del sistema	obligatorio
[op.mon.1] Detección de intrusión	obligatorio
[op.mon.2] Sistema de métricas	obligatorio

Tabla 20 Monitorización del sistema

[mp] Medidas de protección

control	aplica
[mp] Medidas de protección	obligatorio
[mp.if] Protección de las instalaciones e infraestructuras	sí
[mp.if.1] Áreas separadas y con control de acceso	sí
[mp.if.2] Identificación de las personas	sí
[mp.if.3] Acondicionamiento de los locales	sí
[mp.if.4] Energía eléctrica	sí
[mp.if.5] Protección frente a incendios	sí
[mp.if.6] Protección frente a inundaciones	sí
[mp.if.7] Registro de entrada y salida de equipamiento	sí
[mp.if.9] Instalaciones alternativas	sí

Tabla 21. Protección de las instalaciones e infraestructuras

control	aplica
[mp] Medidas de protección	obligatorio
[mp.per] Gestión del personal	sí
[mp.per.1] Caracterización del puesto de trabajo	sí
[mp.per.2] Deberes y obligaciones	sí
[mp.per.3] Concienciación	sí
[mp.per.4] Formación	sí
[mp.per.9] Personal alternativo	sí

Tabla 22. Gestión del personal

control	aplica

[mp] Medidas de protección	obligatorio
[mp.eq] Protección de los equipos	obligatorio
[mp.eq.1] Puesto de trabajo despejado	obligatorio
[mp.eq.2] Bloqueo del puesto de trabajo	obligatorio
[mp.eq.3] Protección de equipos portátiles	sí
[mp.eq.9] Medios alternativos	obligatorio

Tabla 23. Protección de equipos

control	**aplica**
[mp] Medidas de protección	obligatorio
[mp.com] Protección de las comunicaciones	obligatorio
[mp.com.1] Perímetro seguro	sí
[mp.com.2] Protección de la confidencialidad	obligatorio
[mp.com.3] Protección de la autenticidad y de la integridad	obligatorio
[mp.com.4] Segregación de redes	sí
[mp.com.9] Medios alternativos	sí

Tabla 24. Protección de las comunicaciones

control	**aplica**
[mp] Medidas de protección	obligatorio
[mp.si] Protección de los soportes de información	sí
[mp.si.1] Etiquetado	sí
[mp.si.2] Criptografía	sí
[mp.si.3] Custodia	sí
[mp.si.4] Transporte	sí

[mp.si.5] Borrado y destrucción	sí

Tabla 25. Protección de los soportes de información

control	aplica
[mp] Medidas de protección	obligatorio
[mp.sw] Protección de las aplicaciones informáticas (SW)	obligatorio
[mp.sw.1] Desarrollo de aplicaciones	obligatorio
[mp.sw.2] Aceptación y puesta en servicio	obligatorio

Tabla 26. Protección de las aplicaciones informáticas (SW)

control	aplica
[mp] Medidas de protección	obligatorio
[mp.info] Protección de la información	sí
[mp.info.1] Datos de carácter personal	sí
[mp.info.2] Calificación de la información	sí
[mp.info.3] Cifrado de la información	sí
[mp.info.4] Firma electrónica	sí
[mp.info.5] Sellos de tiempo	sí
[mp.info.6] Limpieza de documentos	sí
[mp.info.9] Copias de seguridad (backup)	sí

Tabla 27. Protección de la información

control	aplica
[mp] Medidas de protección	obligatorio
[mp.s] Protección de los servicios	obligatorio
[mp.s.1] Protección del correo electrónico (e-mail)	sí

[mp.s.2] Protección de servicios y aplicaciones web	obligatorio
[mp.s.8] Protección frente a la denegación de servicio	obligatorio
[mp.s.9] Medios alternativos	sí

Tabla 28. Protección de los servicios

4. Conclusión

A lo largo de este capítulo se van a comentar las conclusiones generales extraídas del trabajo realizado en el proyecto Tech4Diet, posteriormente se detallarán propuestas futuras con las que se podrán mejorar el desarrollo del sistema y avanzar en aspectos más genéricos en lo que respecta al proyecto. Finalmente, se expondrán unas conclusiones personales en cuanto al trabajo que se ha realizado a lo largo del proyecto.

4.1. Conclusiones

El trabajo desarrollado en este proyecto ha sido la realización de un sistema de adquisición multicámara RGB-D, necesidad principal para el funcionamiento del sistema de adquisición y modelado del proyecto Tech4Diet, el cual está pensado para su uso en clínicas dietéticas o centros de salud que trabajen en este ámbito; y de una guía de implementación de medidas de seguridad para que el responsable del proyecto pueda tomar decisiones en cuanto a este ámbito se refiere.

De forma más concisa, se han abordado una serie de objetivos específicos que se realizaron durante el desarrollo de este proyecto y que han culminado en los siguientes resultados:

Se ha desarrollado un sistema adquisición multicámara RGB-D utilizando los dispositivos Realsense D435 de Intel, además, esto incluye la elección del entorno de desarrollo software y hardware necesarios, como el SDK que proporciona el manejo de los sensores de los sensores RGB-D y los tipos de cables necesarios para tener un ancho de banda lo suficientemente grande para obtener los datos y no generar cuellos de botella, y el diseño de las vistas que son necesarias para el funcionamiento del sistema.

Para el diseño del desarrollo del sistema de adquisición se ha planteado un diagrama de clases que abarca todos los requerimientos del sistema, lo que nos ha permitido tener un sistema modulable y escalable, que permita implementar futuras extensiones como la posibilidad de utilizar sensores RGB-D de otras marcas de manera transparente.

Este sistema de adquisición se ha puesto en marcha en el conjunto del proyecto Tech4Diet dando un funcionamiento y rendimiento satisfactorio.

Por último, se ha realizado un estudio completo de los aspectos generales y específicos del proyecto Tech4Diet en materia de protección de datos y seguridad. Este estudio permitirá al proyecto salvaguardar, mediante medidas de seguridad, los datos de los pacientes que reciban el servicio ofrecido, protegiendo al proyecto y al personal del mismo, de las posibles penalizaciones por no cumplir la LOPDGDD.

4.2. Líneas Futuras

Por lo que se refiere a líneas futuras a corto plazo, se puede considerar el refinamiento y la optimización de la calidad del dato que se obtienen en el sistema de adquisición multicámara 3D para la posterior construcción del modelo del cuerpo del paciente en el sistema.

De la misma manera, podemos destacar que el responsable de seguridad optimice las medidas de seguridad implementadas actualmente en el proyecto con un plan de acción de mejora continua para cumplir las normativas exigidas del ENS.

Finalmente, se plantea la mejora de la escalabilidad del sistema implementando la funcionalidad para obtener el modelado del cuerpo humano, partiendo de los datos recogidos con sensores de diferentes marcas. Esto le otorga la posibilidad al proyecto que en un futuro se puedan estudiar o analizar dispositivos que ofrezcan mayor rendimiento que los utilizados actualmente.

4.3. Conclusiones personales

Todos los resultados que he obtenido de este proyecto han sido altamente satisfactorios. Empezando desde tener la oportunidad de trabajar en un proyecto de investigación y desarrollo hasta iniciarlo desde cero, asumiendo responsabilidades críticas de primera mano.

Del mismo modo he tenido la posibilidad de aumentar mis conocimientos en la materia de visión por computación y mejorar las habilidades y aptitudes que he desarrollado a lo largo de mi estancia en la carrera.

Por último, tengo que poner de relieve, que gracias al trabajo realizado en este proyecto, del cual me llevo buenos recuerdos y grandes amigos, he podido darme

cuenta de lo preparado que estoy para afrontar los problemas del mundo laboral gracias a las capacidades adquiridas tanto en el proyecto como en la carrera.

Bibliografía

Azorín López, J. (2008). *Modelado de sistemas para visión de objetos especulares inspección visual automática en producción industrial*. https://rua.ua.es/dspace/handle/10045/7751

CCN-STIC. (2017). *Curso GSI - Módulo 5 - Guía de Seguridad de las TIC CCN-STIC 804 ENS. Guía de implantación*. 1–100. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804_medidas_de_implantacion_del_ens.pdf

Cui, Y., Schuon, S., Chan, D., Thrun, S., & Theobalt, C. (2010). 3D shape scanning with a time-of-flight camera. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 1173–1180. https://doi.org/10.1109/CVPR.2010.5540082

Fuster Guilló, A. (2004). *Modelado de sistemas para visión realista en condiciones adversas y escenas sin estructura*. https://rua.ua.es/dspace/handle/10045/9910

Fuster Guilló, Azorín López, Zaragoza, Pérez, Saval-Calvo, & Fisher. (2019). 3D Technologies to Acquire and Visualize the Human Body for Improving Dietetic Treatment. *Proceedings*, *31*(1), 53. https://doi.org/10.3390/proceedings2019031053

Grunnet-Jepsen, A., Winer, P., Takagi, A., Sweetser, J., Zhao, K., Khuong, T., Nie, D., & Woodfill, J. (2018). *Using the Intel ® RealSense TM Depth cameras D4xx in Multi-Camera Configurations*. https://doi.org/10.19729/j.cnki.1673-5188.2018.03.002

Gu, Q., Herakleous, K., & Poullis, C. (2014). *3DUNDERWORLD-SLS: An Open-Source Structured-Light Scanning System for Rapid Geometry Acquisition*. *May 2015*. http://arxiv.org/abs/1406.6595

Khoshelham, K., & Elberink, S. O. (2012). Accuracy and resolution of kinect depth data for indoor mapping applications. *Sensors*, *12*(2), 1437–1454. https://doi.org/10.3390/s120201437

Lazaros, N., Sirakoulis, G. C., & Gasteratos, A. (2008). Review of stereo vision algorithms: From software to hardware. *International Journal of Optomechatronics*, *2*(4), 435–462. https://doi.org/10.1080/15599610802438680

Saval Calvo, M. (2015). *Methodology based on registration techniques for representing subjects and their deformations acquired from general purpose 3D sensors*. http://rua.ua.es/dspace/handle/10045/49990

Schwarz, B. (2010). Lidar: Mapping the world in 3D. *Nature Photonics*, *4*(7), 429–430. https://doi.org/10.1038/nphoton.2010.148

Spain. (2018). Organic Law 3/2018, of fifth of December, on the Protection of Personal Data and guarantee of digital rights. (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales). *Boletín Oficial Del Estado (BOE)*, *294*, 119778–119857. https://doi.org/BOE-A-2012-5403

Villena Martínez, V. (2015). *Análisis comparativo de métodos de calibrado para sensores RGB-D y su influencia en el registro de múltiples vistas*. https://rua.ua.es/dspace/bitstream/10045/48745/8/TFG_VICTOR_VILLENA.pdf